ISSN: 2718-6245

OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Editora: Bib Alejandra Castillo

ISSN: 2718-6245
http://www.esgcffaa.edu.ar/esp/oac-boletines.php
AÑO 3 N° 29
Noviembre 2020

OAC Boletín de Noviembre 2020

"*Un nuevo tipo de guerra ha surgido, en el que la guerra armada ha cedido su lugar decisivo en el logro de los objetivos militares y políticos a otro tipo de guerra —guerra de información—.*"

V. Kvachkov, Спецназ России
http://militera.lib.ru/science/kvachkov_vv/index.html

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), micro-sitio de la **Escuela Superior de Guerra Conjunta**
URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php,.
Es un esfuerzo posible por el financiamiento que el observatorio recibe de la **Universidad de la Defensa Nacional**, a través de los programas UNDEFI y se encuentra inserto en la **Antena Territorial de Defensa y Seguridad** de la Secretaría de Ciencia y Tecnología de la Nación y es administrado por el **Centro de Estudios de Prospectiva Tecnológica Militar "Grl Mosconi" de la Facultad de Ingeniería del Ejército Argentino**
Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial distintas perspectivas de este nuevo ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

ESTRATEGIA

Documento de Interés

Índice de Poder Cibernético

El Índice Nacional de Poder Cibernético (NCPI) de Belfer (Harvard Kennedy School – Center for Science and International Affairs), mide las capacidades cibernéticas de 30 países en el contexto de siete objetivos nacionales, utilizando 32 indicadores de intención y 27 indicadores de capacidad con evidencia recopilada a partir de datos disponibles públicamente. El NCPI ha identificado siete objetivos nacionales que los países persiguen utilizando medios cibernéticos. Los siete objetivos son: (1) Vigilancia y seguimiento de grupos domésticos; (2) Fortalecimiento y mejora de las defensas cibernéticas nacionales; (3) Control y manipulación del entorno de información; (4) Colección de Inteligencia Extranjera para la Seguridad Nacional; (5) Ganancia comercial o mejora del crecimiento de la industria nacional; (6) Destruir o deshabilitar la infraestructura y las capacidades de un adversario;(7) Definición de Normas Cibernéticas y Estándares Técnicos Internacionales.

https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

La Guerra por 5g una mirada estratégica a los datos y la información

Hugo Miguel a través de Infobae presenta la disputa que libran EE. UU. y China gira en torno al control de la información que circula a través de las nuevas redes de comunicaciones móviles. ¿Cómo afecta esto a terceros países y qué debería hacer la Argentina para defender su soberanía digital?

https://www.infobae.com/def/internacionales/2020/10/24/la-guerra-detras-del-5g-la-puja-por-el-control-global-de-la-red-y-el-acceso-a-los-datos/

CIBERDEFENSA

Documento de Interés

Ciberamenazas y Tendencia 2020

En el informe se presentan los elementos más destacables de las amenazas identificadas durante 2019 y principios de 2020, así como las tendencias futuras más relevantes en el ámbito del ciberespacio en España. El tema es tratado desde la perspectiva de los diferentes actores, desde el Estado hasta los insiders, identificando las acciones más significativas, analizando los incidentes más importantes que por su impacto o pueden convertirse en una tendencia. Las operaciones de influencia que se están ejecutando en todo el mundo pueden generar consecuencias directas e indirectas en el corto plazo, proporcionando una visión de lo que sucede en el ámbito local español y en el internacional.

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-58ab18bdb5ae4d67b340eb3a90d39b8c&esid=7a221572-460d-eb11-a813-000d3aab18bd

La ciberdefensa avanzando de cara al futuro

El Ministerio de Defensa de Argentina ha ordenado realizar los estudios correspondientes para la creación de la Competencia de Ciberdefensa en el ámbito de las FFAA y consecuentemente la creación del Instituto de Ciberdefensa de las FFAA, cuyo objetivo será la capacitación del personal militar y civil que las organizaciones de ciberdefensa demandan.

https://www.infobae.com/opinion/2020/11/15/la-ciberdefensa-avanzando-de-cara-al-futuro/

CIBERGUERRA

Interceptación en las redes 5G: una realidad poliédrica

CIBERElcano, nos trae un artículo de Javier Alonso sobre uno de los temas más controvertidos en el ciberespacio, el despliegue de las redes 5G se está llevando a cabo con fuerte apoyo institucional y una atención geopolítica y mediática sin precedentes. Su arquitectura de referencia, protocolos de comunicación e interfaces (interoperabilidad) se concretan en estándares técnicos definidos en el marco de los organismos internacionales especializados. Su definición la lideran agentes del mercado cuya prioridad es el desarrollo de negocio y la hegemonía tecnológica, por lo que la estandarización técnica de aspectos como la ciberseguridad o la interceptación legal, entre otros, no se aborda simultáneamente, con lo que las autoridades policiales y judiciales tienen que buscar *a posteriori* soluciones técnicas y normativas que no son las óptimas mientras los operadores se ven obligados a asumir costes regulatorios adicionales.
http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari117-2020-alonso-ciberseguridad-privacidad-e-interceptacion-legal-en-redes-5g-realidad-poliedrica?utm_source=CIBERElcano&utm_medium=email&utm_campaign=59-oct2020&_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-58ab18bdb5ae4d67b340eb3a90d39b8c&esid=7a221572-460d-eb11-a813-000d3aab18bd

CIBERCONFIANZA

Trabajo remoto y Ransomware

Los meses pasados han puesto al mundo de cabeza, mas no será una novedad para los lectores de este blog saber que el viraje universal hacia el teletrabajo ha cambiado radicalmente el panorama de amenazas. Entre otras cosas, las personas responsables de la ciberprotección corporativa ahora deben considerar dos nuevos factores: la distribución geográfica de la red de oficina y la presencia de las computadoras del trabajo en ambientes domésticos.

https://latam.kaspersky.com/blog/ransomware-telecommuting/18987/?mkt_tok=eyJpIjoiWXpOaE5qTTVaVEkxT0RZNSIsInQiOiJIZ2ZMc1hlRWpZeWpHNm5maVNscXJqMEZNcnB0QmFKWFZUK2pcLzNqM1NDWmI0ZzJYVzEwN05DR0lLRmZ2enB0cTkxTlJyU3FLMWtBQ3F0NW1cL3pWNDFPVVdiTHF3cXFMVW5VVGZiU0xacTNURFdPQW5CNVpvc0tjY2RVTFl3dVYzV0Fvd1NSWWlPckpCakFtdjQzZ0c2QT09In0%3D

CIBERSEGURIDAD

Acciones de Hackeos y ataques de denegación de servicio en la argentina

Se había previsto un festejo cibernético para el 17 de octubre, pero al dar acceso al público comenzó un ataque cibernético, el ataque se produjo bajo la forma de pedido de ingreso de más cantidad de usuarios de los que puede soportar una página, para inutilizarla. Un típico “ataque de denegación de servicios”, que se realiza a través de bots que saturan los puertos de ingreso bombardeando en forma continua información, hasta que logran saturar.

https://www.infobae.com/politica/2020/10/18/decepcion-e-incertidumbre-como-se-vivio-en-el-gobierno-el-fracaso-de-la-movilizacion-virtual-por-el-17-de-octubre/

La ciberseguridad en los aviones comerciales

La Government Accountability Office (GAO) ha instado a la Administración Federal de Aviación a tomar medidas para proteger mejor a los aviones comerciales modernos de los riesgos cibernéticos.

https://www.infosecurity-magazine.com/news/goa-cybersecurity-commercial/

CIBERFORENSIA

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EEUU, estos boletines proporcionan un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad (NVD) del Instituto Nacional de Estándares y Tecnología (NIST)

Semana de 05 de octubre https://us-cert.cisa.gov/ncas/bulletins/sb20-286

Semana de 14 de octubre: https://us-cert.cisa.gov/ncas/bulletins/sb20-293

Semana de 19 de octubre: https://us-cert.cisa.gov/ncas/bulletins/sb20-300

Semana de 26 de octubre: https://us-cert.cisa.gov/ncas/bulletins/sb20-307

Semana del 2 de noviembre: https://us-cert.cisa.gov/ncas/bulletins/sb20-314

Sitio web: http://www.esgcffaa.edu.ar/esp/oac-boletines.php
Nuestra dirección postal es:
* | Luis María Campos 480 - CABA - República Argentina | *
Nuestro correo electrónico:
*|observatorioargentinodelciberespacio@conjunta.undef.edu.ar | *